PRIVACY IMPACT ASSESSMENT (PIA)

For the

Financial Disclosure Management System (FDM)
Office of the Army General Counsel Ethics and Fiscal Division

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 2989 (DA05989)
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier: OGE/GOVT-1 and OGE/GOVT-2

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 7301, 7351, 7353; 5 U.S.C. App. (Ethics in Government Act of 1978); 31 U.S.C. 1353; E.O. 12674 (as modified by E.O. 12731); 5 C.F.R. Part 2634.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

FDM was developed to provide electronic filing, review, and management of a filer's reportable personal financial information in place of completing either an SF 278, Public Financial Disclosure Report, or an OGE Form 450, Confidential Financial Disclosure Report. FDM provides for the secure handling and management of reported information and associated supporting financial documents as required by the financial disclosure regulation (5 C.F.R. Part 2634) of the Office of Government Ethics (OGE) . Such documents include, financial investment status reports, reports concerning agreements between the report filer and prior or future private sector employer, ethics agreements, and the preservation of waivers issued to an officer or employee.

FDM stores the reportable information for review by appropriate agency officials.

Personal information collected/maintained in FDM:
User information: name, grade, address, telephone number, & email address.
Filer information: user information (above) plus official duty position title and reportable financial information required by either the SF 278 or OGE Form 450 (e.g., investments, assets, business relationships).

Agency reviewing officials review the filer's reported information to identify and resolve conflicts of interest between the filer's investments and official duties. The information is retained for six years IAW OGE retention requirements.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Minimal risk to a user's privacy because of system safeguards. No risks in providing an individual the opportunity to object or consent to FDM use. Appropriate safeguards are in place for the collection, use, and safeguarding of personally identifiable information. Risks are further mitigated by the implementation of firewalls, intrusion detection systems and malicious code protection. For security purposes, and to ensure FDM remains available to all authorized users, FDM uses software programs to monitor network traffic, to identify unauthorized attempts to upload or change information, to cause damage, or to deny services. Server logs are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20. FDM has been used increasingly in the Army since 2004. To date, the system safeguards have proven secure and reliable at protecting the reportable personal financial information of all filers as there have been no reported incidents of information compromise.

The scope of the information collection is narrowly tailored to ensure that the information collected matches the uses. The filer self-reports the reportable information ensuring its accuracy.

FDM is a controlled access, role-based system. Only authorized individuals are granted access. Financial disclosure report filers, their assistants, reviewers, their assistants, certifiers and their assistants, and system support personnel are authorized users. Authorized users may have one or more "roles" that affect the user's access and ability to see other users and financial disclosure report information for particular filers.

Department of Defense (DoD) filers use their Common Access Card (CAC) and Personal Identification Number (PIN) for FDM access. Army users may also use their Army Knowledge Online (AKO) account user name and password or CAC card to access FDM. Non-DoD users use their agency's locally maintained directory for user name and password access. Those users' agency password security policies control required password changes.

FDM uses an interface with the DISA Global Directory Service (GDS) (https://dod411.gds.disa.mil) to register and validate a DoD user for access.

Disclosure report filers follow a step-by-step report wizard process to prepare and submit (eSign) the disclosure report form and to attach any necessary/supporting documentation. Once the filer has eSigned the report, FDM

sends email notices to the filer's servicing ethics counselor (EC), the filer's supervisor, and to the report approval/ certifying authority, for appropriate review. Reviewing and certifying authorities use FDM to process the disclosures.

The reported information is retained for six years IAW OGE retention requirements.

An FDM user's data travels between the user's computer Web Browser and FDM servers encrypted by a technology called Secure Sockets Layer (SSL) using 128-bit encryption. This is the same technology banks use and offers the highest level of encryption currently supported by commercial Web browsers. The lock icon in the bottom of the browser window indicates that data is shielded from unauthorized access while in transit. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Web pages that require an SSL connection start with https: instead of http:. Unlike IRS efiling, FDM does not ask for users' social security numbers and bank account number information, yet FDM offers the same security protections that accompany electronic filing of income tax returns.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Information will be available to authorized users with an official need to know in order to perform their official government duties. A Filer's report review chain (e.g., rater/Supervisor and certifying official, as well as authorized assistants) may view the information.

As necessary, appropriate, and when legally permissible, officials in Army components and major commands which includes Active Duty, Army Audit Agency, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army Intelligence and Security Command, Army Reserve Command, Assistant Secretary of the Army (Financial Management & Comptroller), Department of the Army Inspectors General, and the Provost Marshal General may obtain access.

☒ **Other DoD Components.**

Specify. Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that might obtain access to DoD PII in this system, on request in support of an authorized investigation or audit include Defense Criminal Investigative Service, Defense Finance and Accounting Service, Defense Manpower Data Center, Defense Security Service, DoD Inspector General, Office of the DoD Inspector General, and the DoD Defense Information Systems Agency.

☒ **Other Federal Agencies.**

Specify. Information will be available to authorized users in other agencies using FDM with a need to know in order to perform official government duties for that agency's users. The Office of Government Ethics, Veterans Affairs Department, and the Department of Homeland Security are using FDM. A filer's reported information is not shared beyond the filer's agency (except when the filer transers to another agency using FDM).

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

All members of the FDM Project Team (including contractor employees) , Software Engineering Center, CECOM LCMC, that maintain and operate FDM including an FDM Help Desk sign a Confidentiality and Nondisclosure Agreement acknowledging the sensitive nature of the Filer's reported information and agreeing to safeguard it.

MOD 3 of the basic contract added Clause 52.224-01, Privacy Act Notification. This clause state the following: 52.224-1 -- Privacy Act Notification.
As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

Privacy Act Notification (Apr 1984) The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.
(End of Clause)

☐ **Other** (e.g., commercial providers, colleges).

Specify.

INFORMATION IS NOT SHARED WITH ANY NON-GOVERNMENT AGENCIES

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals objecting to the collection of PII refrain from using FDM.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Use of FDM is a user's consent to sharing information with other authorized users. Only select users associated with a particular filer may see that filer's reported financial information. Any authorized FDM user may "search" for another user and find that user's name, email address, and telephone number if/when recorded in FDM's user directory.

The standard DoD Information System Use & Consent notice banner is presented whenever the user tries to login to FDM, https://www.fdm.army.mil/FDM. Contents:

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

User agreement link: https://www.fdm.army.mil/FDM/agreement.html.

The FDM login page includes this Notice:
Financial Disclosure Management (FDM) is a DoD-approved and operated unclassified information system for the electronic filing, reviewing, and managing of required financial disclosure reports. It is a secure, limited access information system. By using it and entering your financial information you acknowledge that authorized users may view your information. Authorized users include your report review chain, assistants you appoint, and FDM administrative personnel. All such personnel are bound by law, regulation, and policy to safeguard your information from unauthorized access and disclosure. In addition, FDM administrative personnel, including Help Desk personnel, execute individual confidentiality and nondisclosure agreements promising not to disclosure your information. Violation of such agreements could lead to disciplinary action.

A Privacy Act Statement is on the FDM website: https://www.fdm.army.mil/FDM/privacy.html.

Use of the FDM system constitutes consent to the specific uses of the information collected.

(2) If "No," state the reason why individuals cannot give or withhold their consent.